

Firewall

A firewall is a system designed to prevent unauthorized access to or from network segments. Sessions passing through the firewall are matched against specified security criteria to determine if the sessions should be allowed or blocked.

Superior Performance and Protection

A firewall is an essential security component in any organization with network implementations, which require segmentation and access control between networks. The challenge of meeting these requirements has increased with the rise of new threats and evasive applications, ever-increasing traffic volume, and the mobile nature of network endpoints.

FortiOS firewall features and FortiGate hardware acceleration keep pace with this new reality. Utilizing the unique FortiASIC processor, a FortiGate delivers outstanding performance with high throughput and ultra-low latency, while meeting an organization's budget. Its robust firewall policy implementation extends traditional IP address control with user and device awareness. Administrators can also easily apply additional security measures on policies using a variety of security profiles such as AV, IPS, and application control, along with traffic shaping behavior, NAT settings, and more.

Managing policies using FortiOS is easy, even with thousands of rule sets. Administrators can work on the dynamic policy table using contextual menus and drag-and-drop features, while intelligent search and a variety of annotation capabilities allow the user to quickly find and organize desired policies.

Key Features & Benefits

Superior price-performance using hardware acceleration	Allows the organization uncompromised security implementation within budget.
Robust firewall policy implementation with user and device awareness	Provides the ability to secure today's network, which includes mobile users and devices.
Enterprise-grade policy management	Allows easy management of complex policy requirements minimizing configurations errors.

Cutting edge, high performance access control and protection for your valuable assets.

- Utilizes hardware acceleration technologies to meet high traffic load with low TCO.
- Proven protection with over 200,000 customers worldwide.
- Enterprise class policy management capabilities.

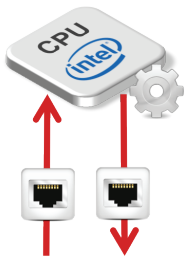


Certified Protection & Performance

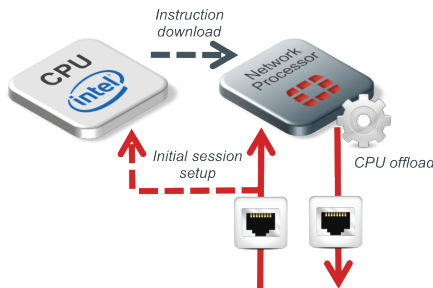
External testing and validation of products is an integral part of Fortinet's product life cycle. As new platforms and functionality are introduced, third-party labs continue to ensure that FortiOS adheres to evolving standards.

With the greatest number of certifications in the market, the FortiOS firewall component provides quality protection to nearly 200,000 customers. FortiOS continuously receives globally recognized NDPP - Common Criteria (CC) certifications, and is enrolled into evaluation by independent external NSS public tests. These independent certifications demonstrate the ability of FortiOS to meet the highest standards of performance and accuracy.

Legacy Security Gateway Appliances



FortiGate with FortiASIC



Outstanding Performance with Hardware Acceleration

Traditional security appliances that use multi-purpose CPU-based architectures typically become an infrastructure bottleneck. The only method of scaling a network security appliance is to use application-specific integrated circuits (ASICs) that accelerate packet processing. Optimum path processing (OPP) is then used to optimize the different resources available in packet flow.

FortiOS handles the initial session setup via CPU, with subsequent packets that are offloaded to one or more FortiASIC Network Processors (NP), which have received instructions from the CPU. This offload improves throughput capacity and latency, and also releases the CPU from overload, thereby increasing platform stability. In addition, due to FortiASIC's acceleration, performance is consistent across all packet sizes. This is extremely useful as traditional appliances have significant difficulties dealing with today's small packet sizes found in streaming media and VoIP traffic.

Flexible Deployment Modes

Fortinet recognizes the desire for organizations to deploy consistent platforms for ease of management and lower TCO across various network infrastructures. FortiOS has the flexible capabilities to address these needs. The firewall is able to operate in traditional route mode as well as transparent bridge mode. When deployed with VDOMs (virtual domains), organizations can enjoy hybrid mode where both route and transparent modes are operating concurrently in a single device.

FortiOS supports major routing protocols and intelligent policy routing for allowed traffic in route mode while capable of interoperating with most Layer 2 protocols, such as Spanning Tree Protocol (STP) in bridge mode.

User and Device Awareness

Most networks in today's organizations are connected with both corporate and personal mobile devices. User and device awareness provides the option of configuring intelligent policies that can effectively enforce security.

To tackle the prevalence of BYOD environments, administrators are able to configure policies with sources defined by IPs, users, and devices, either combined or selectively.

Robust Policy Management

Powerful policy management is critical in enforcing an organization's complex, yet granular security requirements. The ease of use is equally important for minimizing configuration errors.

FortiOS offers the unique section view and global view modes when presenting the policy table. These modes provide familiarity to experienced administrators who may be well-versed in either design. You can further customize the policy table by configuring the column items displayed. Pictograms and icons also improve visualization of the configurations.

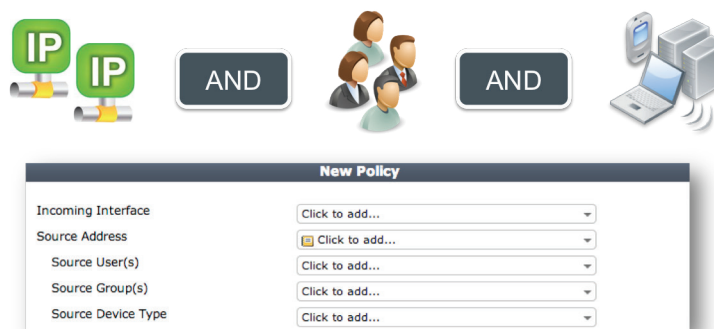
Administrators can perform a wide variety of policy manipulation on the policy table itself without switching between configuration panels. These functions include:

- Editing, adding, removing, cutting, and pasting objects or complete policies
- Arranging policies and column items using drag-and-drop
- Changing policy actions and features, such as enabling NAT
- Showing object references
- Dragging and dropping objects between policies

FortiOS allows administrators to quickly locate or to filter policies and objects on the policy table with a smart search bar and column filters. Administrators can also add comments and associate objects with colored icons and tags.

Comprehensive Policy Objects

FortiOS provides a wealth of policy objects to empower administrators when setting up granular policies. For example, organizations can use GeoIP addresses to dynamically block terminals from certain geography.



Broad NAT Support

Network Address Translation (NAT) is an essential network feature that is often associated with firewalls operating in Layer 3 mode. Apart from providing a simple means of security, NAT is often used by service providers to address IPv4 depletion or IPv6 transition.

FortiOS supports various standard NAT types, such as different favors of static (one-to-one) and dynamic (one-to-many) NAT implementations, including full-cone NAT and port forwarding. FortiOS also supports a central NAT table, as well as NAT for VPNs and VoIP/media protocols.

FortiOS offers various CGN (Carrier grade NAT) for service providers such as NAT46, NAT64, NAT66, and PBA (Port Block Allocation) NAT.

Extensive Network Protocol Support

Today's networks might require support for a variety of network protocols that provide the best options to different environments. FortiOS supports various network and transport layer protocols such as TCP, UDP, SCTP, GTP, and ICMP. It is also able to handle complex applications using configurable session helpers that include H.245, H.323, MGCP, SIP, and more.

FortiOS provides extensive multicast firewalling capabilities suitable for protecting IP surveillance and media broadcasting networks. It supports PIM sparse mode (RFC 4601) and PIM dense mode (RFC 3973), and can service multicast servers or receivers on the network segment to which a FortiGate unit interface is connected.

FortiGate® - High performance Network Security Platform

• ASIC-Powered Performance

FortiGate purpose-built hardware delivers unmatched price/performance for the most demanding networking environments. FortiASIC processors ensure that your network security solution does not become a network bottleneck.

• High speed and Flexible Connectivity

The FortiGate product family offer a variety of interfaces for today's network, ranging from integrated WAN interfaces, 3G/4G USB wireless broadband support to high speed 40G interfaces for data centers.

• Broad Product Offerings

The FortiGate product family scales from desktop units for remote branch offices, mid-range for small and medium enterprises to high-end platforms for service providers and data centers

#	Date/Time	Source	Device	Destination	Application Name	Security Action	Security Events	Sent / Received	Action	Threat Score
1	14:55:05	Administrator (10.170.203.3)	xyz-pc	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	876 B / 3.34 KB	close	335544325
2	14:55:04	demouser (10.170.203.3)	abc-laptop	208.83.222.148	BitTorrent	Allowed	APP 1 APP 2	95 B / 0 B	accept	335544325
3	14:55:04	demouser (10.170.203.3)	abc-laptop	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	904 B / 3.75 KB	close	
4	14:54:59	Administrator (10.170.203.3)	xyz-pc	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	876 B / 3.34 KB	close	
5	14:54:59	demouser (10.170.203.3)	abc-laptop	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	904 B / 3.75 KB	close	
6	14:54:58	demouser (10.170.203.3)	abc-laptop	95.24.252.241	BitTorrent	Allowed	APP 1 APP 2	95 B / 0 B	accept	335544325
7	14:54:57	demouser (10.170.203.3)	abc-laptop	208.91.112.53	DNS	Allowed	APP 1 APP 2	59 B / 356 B	accept	
8	14:54:54	Administrator (10.170.203.3)	xyz-pc	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	876 B / 3.34 KB	close	
9	14:54:54	demouser (10.170.203.3)	abc-laptop	157.55.235.148	Skype	Allowed	APP 1 APP 2	1.09 KB / 2.63 KB	accept	335544325
10	14:54:54	demouser (10.170.203.3)	abc-laptop	157.55.235.140	Skype	Allowed	APP 1 APP 2	261 B / 552 B	accept	335544325
11	14:54:53	demouser (10.170.203.3)	abc-laptop	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	904 B / 3.75 KB	close	
12	14:54:52	demouser (10.170.203.3)	abc-laptop	213.199.179.146	Skype	Allowed	APP 1 APP 2	187 B / 119 B	accept	335544325
13	14:54:51	demouser (10.170.203.3)	abc-laptop	94.28.170.119	BitTorrent	Allowed	APP 1 APP 2	95 B / 98 B	accept	335544325
14	14:54:49	Administrator (10.170.203.3)	xyz-pc	173.212.140.80 (cbbs.fortiguard.com)	HTTP.BROWSER	Allowed	APP 1 APP 2	876 B / 3.34 KB	close	
15	14:54:48	demouser (10.170.203.3)	abc-laptop	97.89.170.108	10964/UDP	Allowed	APP 1 APP 2	46 B / 54 B	accept	
16	14:54:48	demouser (10.170.203.3)	abc-laptop	96.32.66.214	39175/UDP	Allowed	APP 1 APP 2	46 B / 54 B	accept	
17	14:54:48	demouser (10.170.203.3)	abc-laptop	192.66.173.188	39175/UDP	Allowed	APP 1 APP 2	46 B / 54 B	accept	

Monitoring, Logging, and Reporting

FortiOS empowers an organization to implement security best practices that require continuous monitoring of threats, allowing the organization to adapt to new requirements.

The FortiView dashboards display useful analysis data with detailed and contextual session information, which can be filtered and ranked, with drilldown options also available. This information, including system events activities and administration audit trails, can also be archived via logs.

FortiOS logs all the types of traffic that can connect to or terminate at the FortiGate unit. In turn, these logs can generate useful trending and overview reports.

FortiOS also offers robust in-built e-mail and SMS alert systems, which can integrate with external threat management systems such as SNMP and standard based syslogs.

ADDITIONAL REFERENCES

Resource	URL
The FortiOS Handbook - The Complete Guide	http://docs.fortinet.com/fgt.html
Fortinet Knowledge Base	http://kb.fortinet.com/
Product Datasheets & Matrix	http://www.fortinet.com/resource_center/datasheets.html
Fortinet Solution Page	http://www.fortinet.com/solutions



GLOBAL HEADQUARTERS	EMEA SALES OFFICE	APAC SALES OFFICE	LATIN AMERICA SALES OFFICE
Fortinet Inc. 899 Kifer Road Sunnyvale, CA 94086 United States Tel: +1.408.235.7700 Fax: +1.408.235.7737	120 rue Albert Caquot 06560, Sophia Antipolis, France Tel: +33.4.8987.0510 Fax: +33.4.8987.0501	300 Beach Road #20-01 The Concourse Singapore 199555 Tel: +65.6513.3730 Fax: +65.6223.6784	Prol. Paseo de la Reforma 115 Int. 702 Col. Lomas de Santa Fe, C.P. 01219 Del. Alvaro Obregón México D.F. Tel: 011-52-(55) 5524-8480

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.